U.S. Department of Agriculture

Office of Inspector General
Western Region

Audit Report

Natural Resources Conservation Service
Water and Climate Information System
Review of Application Controls
Portland, Oregon

Report No. 10501-1-SF
December 2004

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

DATE: DEC 15 2004

REPLY TO
ATTN OF: 10501-1-SF

SUBJECT: NRCS Water and Climate Information System - Review of Application Controls

TO: Bruce I. Knight
Chief
Natural Resources Conservation Service

ATTN: Steve Probst
Acting Director
Operations Management and Oversight Division

This report presents the results of our review of the application controls of the Natural Resources Conservation Service's (NRCS) Water and Climate Information System. Your October 27, 2004, response to the draft report is included in exhibit A, with excerpts and the Office of Inspector General's position incorporated into the relevant sections of the report.

Based on the written response, we have accepted NRCS' management decision for all audit recommendations, except for Recommendations 1 and 6. We will be able to accept your management decision for Recommendations 1 and 6 when you provide us with additional information as outlined in the OIG Position section of the report.

In accordance with Departmental Regulation 1720-1, please furnish a reply within 60 days providing the information requested for Recommendations 1 and 6. Please note that the regulations require a management decision to be reached on all the findings and recommendations within a maximum of 6 months from report issuance. Follow your internal agency procedures in forwarding final action correspondence to the Office of the Chief Financial Officer.

/s/
ROBERT W. YOUNG
Assistant Inspector General
for Audit

Executive Summary

Natural Resources Conservation Service Water and Climate Information System - Review of Application Controls (Audit Report No. 10501-1-SF)

Results in Brief

This report presents the results of our audit of application controls within the Natural Resources Conservation Service's (NRCS) Water and Climate Information System (WCIS). Application controls are the measures an organization takes to provide for the safety, accuracy, and completeness of data within its information systems. Although, our review did not identify any concerns with the accuracy and completeness of data, we determined that management controls over system security were inadequate, leaving valuable data vulnerable to unauthorized access and alteration.

Our audit disclosed conditions that need management action. Specifically, risk assessments were conducted according to outdated regulations. Security plans were not timely updated. Contingency plans to recover operations of WCIS in the event of major systems failures were not complete. The system had not been properly accredited or certified. Of most immediate concern, medium- and high-risk vulnerabilities should have been identified and mitigated as part of required periodic scanning.

During conversations regarding these issues, the Chief Information Officer (CIO) (responsible for NRCS information systems) recognized that the agency lacked a mechanism to ensure that personnel were made aware of the relevant regulations (and changes to them). Such a control mechanism would provide the most up-to-date guidance available to personnel responsible for implementing regulations.

In addition, the agency lacked a management oversight system that would—as a matter of course—involve the CIO in monitoring that the regulations were timely and properly implemented. For the risk vulnerabilities in the WCIS, such monitoring would have informed the CIO that field level personnel were not doing required tasks.

Recommendation In Brief

Establish controls to ensure that Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST), and Departmental Information Technology (IT) security requirements are met, especially in the development of disaster recovery and security plans, risk assessments and the performance of vulnerability scans for all field units.

Agency Response

In its written response to the official draft report, dated October 27, 2004, NRCS generally concurred with the audit findings and recommendations. The complete written response is shown in exhibit A of the audit report.

OIG Position

Based on NRCS' written response, OIG accepts NRCS' management decision for all audit recommendations, except for Recommendation Nos. 1 and 6. Additional information is needed in order to reach management decision on the two remaining recommendations.

Abbreviations Used in This Report

Center	National Water and Climate Center
CIO	Chief Information Officer
CS	Cyber Security (issued by OCIO)
GAO	Government Accountability Office
ISS	Information System Security
ISSPM	Information System Security Program Manager
IT	Information Technology
NRCS	Natural Resources Conservation Service
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
USDA	United States Department of Agriculture
WCIS	Water and Climate Information System

Table of Contents

Background and Objectives

Background

USDA's Office of the Chief Information Officer (OCIO) is responsible for establishing, implementing, and overseeing a departmental-wide information security program, while the component agencies are responsible for the day-to-day management of information security for their mission-support systems. During 1999, USDA's Office of Inspector General and Government Accountability Office (GAO) found significant information security weaknesses at the Department's two major data centers, which placed critical assets at significant risk.

In August 2000, the GAO released a report on USDA's information security to the Chairman, Subcommittee on Department Operations, Oversight, Nutrition, and Forestry, Committee on Agriculture, House of Representatives. The report, "USDA Needs to Implement Its Departmental-wide Information Security Plan," states that automated systems are essential to USDA's operations and the delivery of its mission-critical programs, especially as it moves towards electronic government (e-government).

One critical asset is NRCS' Water Climate Information System (WCIS). WCIS is an extensive, automated system designed to collect snow pack and related climatic data in the western United States. The system evolved from NRCS's congressional mandate in the mid-1930's to measure snow pack in the mountains of the West and forecast the water supply. The program began with manual measurements of snow courses, but since 1980 it has relied on an automated system that has collected the data needed to produce water supply forecasts and to support the resource management activities of NRCS and others.

The WCIS provides information related to climate studies, air and water quality investigations, and water resource management concerns. The high-elevation watershed locations and the broad coverage of the network provide important data collection opportunities to researchers, water managers, and emergency managers for natural disasters such as floods.

WCIS is maintained by NRCS' National Water and Climate Center, located in Portland, Oregon. All data received by the WCIS central computer is linked to the Centralized Forecasting System where the public can access the data via the Center's homepage.

USDA follows Federal systems security requirements set forth by the Office of Management and Budget (OMB). The National Institute of Standards and Technology (NIST) interprets OMB's requirements and issues guidance to foster compliance. USDA's OCIO passes the requirements and guidance to the agencies within the Department and ensures that the Federal requirements

are met. Within NRCS, the CIO is responsible for informing field units of the OMB requirements and establishing controls to ensure the units respond to Department oversight and report to the OCIO on the status of systems security.

Objective

Our audit objective was to determine if the Water and Climate Information System's application controls are in place and are functioning to provide for accuracy, and completeness of system data. Our review did not identify any problem with the completeness and accuracy of the data once it was collected.

During this audit, we expanded our original objective to: 1) determine if it was properly secured against unauthorized access and if its data was adequately protected from unauthorized alteration, and 2) assess the adequacy of management oversight of system security.

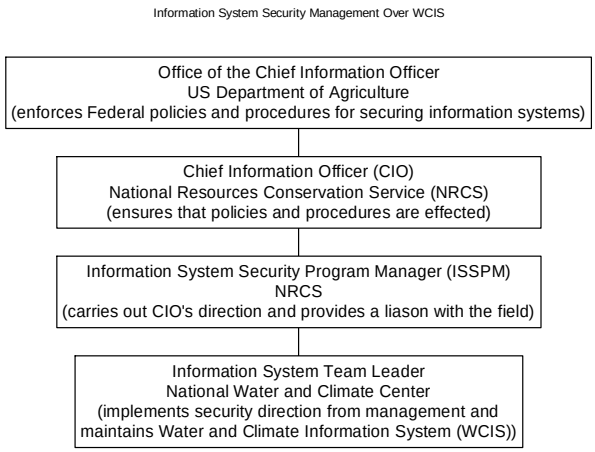
Findings and Recommendations

Section 1. Management Oversight

Finding 1 — NRCS Did Not Maintain Oversight or Control Over WCIS

The information in NRCS' Water and Climate Information System (WCIS) has neither been adequately secured from threats to data integrity, nor appropriately prepared to recover in the event of major system failure. Although there is a wealth of Federal and Departmental guidance designed to obviate these concerns, NRCS' Chief Information Officer (CIO), due to a variety of circumstances described below, did not have controls in place to affect the appropriate policies and procedures, or to monitor their implementation. As a result, the agency cannot be assured of the integrity of data used, for example, by farmers to prepare for drought, emergency workers to anticipate flooding, and reservoirs to manage water reserves.

Following Federal regulation, the Department level OCIO enforces Federal policies and procedures for securing information systems. The OCIO distributes its guidance to the agency level NRCS' CIO who bears overall responsibility for making sure that it is put into practice within the agency. Following the OCIO's lead, NRCS' CIO should disseminate the requirements—either directly or through NRCS's Information System Security Program Manager (ISSPM)—to information systems team leaders in the field who carry out the security instructions. The team leaders should then communicate back up through the chain of command so that the CIO can ensure that the systems are secured according to regulation.



Our audit determined that NRCS' CIO did not provide the field level team leader with OCIO direction regarding contingency plans, security plans,

system certification, and risk assessments (see finding 2 below). In addition, when there were OCIO instructions provided to scan the Water and Climate Information System each month, the CIO did not maintain management oversight to make certain that the job was done. As a result, the system was not properly secured. When we scanned the system during our audit, we found two high-risk and one medium-risk vulnerability that could have been exploited to gain access to sensitive data and possibly allow the system to be compromised. The details are described in Finding 3 of this report.

Recommendation No. 1

Establish controls to communicate Federal and Department level security guidance to field level units and develop an oversight system to ensure compliance.

Agency Response.

NRCS' response stated that the CIO does not have direct line authority to direct, control, and manage operations of the WCC (National Water and Climate Center). The response added that this issue is a leadership call to address, mitigate, and correct as leadership deems appropriate.

OIG Position.

NRCS' response did not address the audit recommendation. In order to reach management decision, NRCS needs to provide OIG with the specific controls that NRCS plans to establish that will communicate all NIST and USDA security requirements to the field level units as well as the timeframes when the controls will be implemented.

Without proper controls, the Water and Climate Information System is at risk of being compromised. As previously described, NRCS' CIO is responsible for effecting and monitoring the agency's information system security but did not have adequate mechanisms in place to communicate Department level security guidance to the field level where that guidance is implemented. As a result at that time of our audit, the Water and Climate Information System was not adequately secured.

Finding 2 Preventive Security Measures Did Not Meet Requirements

The National Water and Climate Center (Center) did not properly prepare to recover the WCIS in case of disaster, update security plans to safeguard the WCIS, certify the WCIS, or assess the WCIS for risks. In each case, information system team leader stated that he had not been made aware of security requirements (or changes to the requirements). Without the safeguards developed by the Department to protect it from known risks, NRCS' WCIS remained unnecessarily vulnerable and less likely to recover should its vulnerability be exploited.

The Office of Management and Budget (OMB) Circular A-130 sets general Federal security requirements for information systems, and the National Institute of Standards and Technology (NIST) issues guidance that translates those requirements into more specific steps[1] (OMB A-130 states agencies must implement NIST guidance) Departmental requirements (manuals, directives, etc.) further formalize these rules into policies and procedures.

Our audit determined that several security measures undertaken by the Center did not meet the above requirements.

Contingency Plans

OMB A-130[2] requires agencies to plan for how they will continue to perform their mission or recover from the loss of application support in the event of a system failure. NIST[3] states that general support systems require contingency plans. It also states that contingency plans should be tested since untested or outdated contingency plans create the false sense of a system's ability to recover in a timely manner.

[1] OMB A-130, Appendix III, dated November 30, 2000.
[2] OMB A-130, Appendix III, dated November 30, 2000.
[3] NITS SP 800-18, Guide for Developing Security Plans for IT Systems, dated December 1998.

Cyber Security (CS) -028[4] issued by the OCIO requires the agency to develop and implement an executable IT Disaster Recovery Plan for each critical application. NIST[5] specifies that Disaster Recovery Plans apply to major, usually catastrophic, events that deny access to the normal facility for an extended period, and for disruptions that require relocation.

WCIS' contingency plan did not indicate how the agency intends to recover the system in the event of catastrophic system failure. NRCS' CIO said that due to workload and other priorities, she was unable to monitor the contingency plan development to ensure that was progressing as required by OMB and NIST regulations. The CIO did state that NRCS is negotiating with a contractor to develop an appropriate disaster recovery site, but the contract had not been signed as of the date of our review. In addition, the information systems team leader said that the team was in the process of getting the disaster recovery plan completed by April 2005.

Security Plans

OMB A-130 requires agencies to prepare a security plan. According to NIST,[6] there should be a policy that requires the production, update, and review of system security plans on a periodic basis or when the systems are implemented or significantly changed. CS-025[7] requires all Security Plans be submitted to the OCIO by April each year.

The Center did have one overall general security plan for its network, but the security plan was not properly reviewed, approved, updated, or submitted annually.

- The security plans for WCIS lacked documentation that indicated who approved the changes (name and title of approving management official and date of approval). The information systems team leader stated he was not aware that the security plans needed formal written certification and approval whenever updates and changes were made.

- The Center did not have a policy that required updates and review of system security plans on a periodic basis. Although the Center had security plans there was no evidence indicating that it had periodically reviewed the security plans since 2001.

[4] CS-028, IT Contingency and Disaster Planning, dated 5/23/03, Referenced to DR 3500, Chapter 14..
[5] NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, dated June 2002.
[6] NIST SP 800-18, Guide for Developing Security Plans for IT Systems, dated December 1998.
[7] CS-025, Cyber Security Plan, dated March 31, 2003 Referenced to DM 3500, Chapter 13.

NRCS' CIO confirmed our determination that due to workloads and other priorities, controls had not been established to ensure that the security plan was updated according to NIST guidelines and that the updated plan was submitted to the Department on an annual basis.

Certification and Accreditation

OMB Circular A-130[8] states that accreditation of a system to process information provides an important quality control. The USDA Certification and Accreditation Guide[9] requires agencies to ensure that a management official authorizes the use of each system before beginning or significantly changing processing in the system. Use of the system must be re-authorized at least every 3 years.

Although WCIS has been in use since 1980, the system had not been certified and accredited. The information system team leader was unaware of the requirement until September 2003 at which time a contract was written to have this work done. Subsequently, the CIO directed the Center to certify and accredit WCIS, and the team leader informed us that he anticipates completion in September 2004.[10]

Risk Assessments

NIST's October 2001 Risk Management Guide requires that a risk assessment include: "1) the identification of threats and vulnerabilities; 2) the identification and analysis of security controls; 3) the analysis of impact or magnitude of harm that a loss of confidentiality, integrity, or availability would have on operations (including mission, functions, image, or reputation), assets, or individuals; 4) the likelihood of threat exploitation of vulnerabilities; and 5) determination of risk."[11] CS-031[12] states that a formal system risk analysis is required every three years or when a major change in made in a system. Major changes are defined as modifications to the system that affect the security controls and which render the system vulnerable to compromise or intrusion.

In 2002, when Center staff conducted a risk assessment for WCIS, they did not do so according to the above NIST requirements. Instead, they relied on a previous assessment prepared by a contractor before the October 2001 requirements were in place. When we questioned the CIO about the risk assessment, she stated that she had not established controls to ensure that risk assessments had been properly completed.

[8] OMB A-130, Appendix III, Section B(a)4, dated November 2000.
[9] USDA Certification and Accreditation Guide, dated June 2, 2003.
[10] OMB recently tied C&A to budget (funding) availability and the USDA set a goal of having all systems certified and accredited by 9/30/04
[11] NIST SP 800-30, dated October 2001
[12] CS-031, Chapter 8, Risk Management Program, dated July 7, 2003

Overall, the CIO did not communicate current policies and procedures to field level staff responsible for implementation. During our review, we found that WCIS had issued a contract to have an independent contractor develop the contingency plan, security plan and risk assessment by June 30, 2004, so that the WCIS can be certified and accredited by September 30, 2004.

Recommendation No. 2

Develop a disaster recovery plan in accordance with OMB and NIST requirements as part of the contingency plan and test the complete contingency plan once developed.

Agency Response.

The WCIS Certification and Accreditation was completed on September 30, 2004, with the IT Contingency/Disaster Recovery Plan testing being completed in April 1, 2005.

OIG Position.

We accept NRCS' management decision on this recommendation. The estimated final action date is April 1, 2005.

Recommendation No. 3

Establish a formal approval process for security plans that documents the name and title of the approving management official and the date of approval and follow Departmental Regulations.

Agency Response.

The NRCS IRM Security Manual and the National IRM Manuals are scheduled for review and updates in accordance with current Departmental policy and NIST guidance. Both manuals will incorporate language relative to Certification and Accreditation, by December 30, 2004.

OIG Position.

We accept NRCS' management decision on this recommendation. The estimated final action date is December 30, 2004.

Recommendation No. 4

Implement procedures requiring that the security plan be reviewed, updated, and certified per NIST guidelines and that updated plans be submitted to the OCIO on an annual basis.

Agency Response.

The NRCS IRM Security Manual and National IRM Manuals are scheduled for review and updates in accordance with current Departmental policy and NIST guidance. Both manuals also will incorporate language relative to Certification and Accreditation and Security Plan updates, by December 30, 2004.

OIG Position.

We accept NRCS' management decision for this recommendation. The estimated final action date is December 30, 2004.

Recommendation No. 5

Perform a Certification and Accreditation (C&A) on the WCIS system per OMB regulations and USDA guidance.

Agency Response.

The Certification and Accreditation on WCIS was completed on September 30, 2004.

OIG Position.

We accept NRCS' management decision for this recommendation. The final action date was September 30, 2004.

Recommendation No. 6

Establish controls to ensure that use of the WCIS system is reauthorized every 3 years.

Agency Response.

Once Certification and Accreditation for WCIS is completed, NRCS will work on a continual basis to ensure that WCIS is reauthorized every 3 years according to USDA and NIST policies and regulations.

OIG Position.

In order to reach management decision on this recommendation, NRCS needs to provide an estimated completion date on when the controls will be established.

Recommendation No. 7

Complete risk assessments of the WCIS that will meet NIST, OMB and USDA requirements.

Agency Response.

The NRCS security team conducted a Risk Assessment on WCIS during July 2004, and will maintain these requirements per USDA and NIST policies and regulations.

OIG Position.

We accept NRCS' management decision on this recommendation. The final action date was July 2004.

Finding 3 Vulnerability Scans Not Conducted

Monthly vulnerability scans of the WCIS were not conducted (vulnerability scans analyze a computer system to identify well-known security weaknesses). The Center's staffs had guidance requiring them to perform these scans on a monthly basis, but they were not performing them. Since the CIO did not have an oversight mechanism in place (e.g., monthly reporting of scan results), the lack of compliance continued until the time of our audit. Without the scans to timely identify serious weaknesses, the system had a significant risk of being compromised.

USDA Departmental Manual[13] states, information system security (ISS) scanner software will be run on a monthly basis on all computer systems. Cyber Security Policy and Procedure[14] states agency management or the CIO will ensure that all agency/staff offices order and use the software to conduct ISS scans on a monthly basis.

In February 2004, we interviewed the information systems team leader and learned that the Center had just completed its first ISS scan of WCIS. The team leader stated that there had been no guidance from the CIO to make sure that the monthly scans were done.

On February 23, 2004, the day we arrived to begin our audit—Center staff obtained the scanning software which had been available since 2001 and ran the vulnerability scan. The software detected two high-risk vulnerabilities

[13] Departmental Manual 3500-002, Chapter 6, dated April 4, 2003.
[14] OCIO CS-007, dated September 5, 2001

and one medium-risk vulnerability.[15] We confirmed their results during two separate scans in March 2004.

Recommendation No. 8

Require responsible officials to timely submit verification to the CIO that monthly vulnerability scans have been run on WCIS.

Agency Response.

A monthly report on scan activity will be reported to the CIO by the NRCS ISSPM. The action is to be completed by December 30, 2004.

OIG Position.

We accept NRCS' management decision on this recommendation. The estimated final action date is December 30, 2004.

Recommendation No. 9

Take immediate action to correct the high- and medium-risk vulnerabilities identified by the scans and conduct an immediate rescan to ensure that the vulnerabilities have been corrected.

Agency Response.

On the two high-risk vulnerabilities identified by the scanning software: a) one was found to be a false positive indicating the vulnerability did not exist, and (b) the second high-risk vulnerability involved the presence of system services, which are required to meet a business requirement and function of WCIS. This vulnerability was mitigated by ensuring that no shell interpreters were in the root/cgi-bin, in accordance with the accepted security practices, and this mitigation was in place at the time of the scans. On the medium vulnerability, it also involved the existence of a required service running on the e-mail server. This e-mail server has been patched to mitigate this medium vulnerability.

OIG Position.

We accept NRCS' management decision for this recommendation. The final action date was October 2004.

[15] High-risk vulnerabilities are those that could allow access to the computer and possibly to the network of computers. Medium-risk vulnerabilities are those that could allow access to sensitive network data that may lead to exploitation of other vulnerabilities

Scope and Methodology

For this audit, we reviewed the adequacy of application controls over the Center's WCIS network. We selected the WCIS for review because the parent agency, NRCS, had identified this system as a major application needing to be certified and accredited.

This audit of NRCS is part of a nationwide audit of USDA mission-critical systems. A nationwide audit report will be issue to the Department's Office of the Chief Information Officer by OIG's Financial and Information Technology Operations and might include sections of this report.

This review was performed at NRCS' Center located in Portland, Oregon. Fieldwork was performed from February 23, 2004, through March 25, 2004.

Our review included an evaluation of the data within the WCIS to determine if it was complete and accurate once it was collected by the sensors located in the snow pack in the mountains. We did not evaluate the sensors themselves to determine their reliability at the collection stage. Our review did not identify any problems or concerns with completeness and accuracy of the data once it was collected.

During the audit, we expanded out objective to review the overall security of system data, including management oversight of system security.

To accomplish our audit objectives, we performed the following audit steps and procedures:

- We reviewed IT security policies and procedures from the Department's Office of the Chief Information Officer, OMB, NIST, and USDA Departmental Manual.

- We interviewed responsible NRCS officials managing the WCIS.

- We performed ISS vulnerability scans on the WCIS.

- We analyzed records and controls (Contingency Plan, Security Plan, Risk assessment and Certification and Accreditation Process) established to ensure the data integrity of the WCIS.

This audit was performed in accordance with generally accepted government auditing standards.

United States Department of Agriculture

NRCS

Natural Resources Conservation Service
P.O. Box 2890
Washington, D.C. 20013

OCT 27 200

SUBJECT: MGT – Natural Resources Conservation Service - Water and Climate Information System – Review of Application Controls (105-1-SF)

TO: Robert W. Young
Assistant Inspector General for Audit
Office of the Inspector General

File Code: 330-12

Attached are the Natural Resources Conservation Service written responses for management decisions on the above cited audit.

If you have questions regarding this response, please contact Steven Probst, Soil Conservationist, Operations Management and Oversight Division, at (202) 720-8208.

Dana D. York for
BRUCE I. KNIGHT
Chief

Attachment

cc:
Dana D. York, Associate Chief, NRCS, Washington, D.C.
P. Dwight Holman, Deputy Chief for Management, NRCS, Washington, D.C.
Katherine C. Gugulis, Deputy Chief for Strategic Planning and Accountability, NRCS, Washington, D.C.
Mary P. Thomas, Chief Financial Officer and Director, Information Technology Division, NRCS, Beltsville, Maryland

The Natural Resources Conservation Service provides leadership in a partnership effort to help people conserve, maintain, and improve our natural resources and environment.

An Equal Opportunity Provider and Employer

Background Information:

The Natural Resources Conservation Service (NRCS) is a decentralized organization with a line and staff hierarchy. Many organizational units with major Information Technology (IT) functions do not come under the direct authority and ambit of the Chief Information Officer (CIO). The Water and Climate Center (WCC) is an example of this hierarchy. Jon Werner, National Hydraulic Engineer, is the management official responsible, within the organization, for the management and oversight activities of WCC. The CIO is responsible for providing the information and guidance for IT security policies and procedures.

Guidance and policies are already established within the National Information Resources Management (IRM) Manual and the National Information Security Handbook. Particularly, detailed information is provided in Part 608 – Business Continuity Planning (National Security Handbook), which states the primary purpose of the Business Continuity Plan "is to provide for the protection and restoration of IT facilities and capabilities, and to reduce the damaging consequences of any unexpected or undesirable event…and procedures apply to all operations in the office." Further, preparing a Business Continuity Plan "provides an excellent opportunity to identify and minimize potential problems that could disrupt operations."

The CIO provides regular and periodic guidance to all units, in the form of communiqués, manual updates, and "tips and techniques" to enhance and improve security controls. NRCS also has an online Directives System, which is available, and can be utilized to provide timely guidance to employees and others.

Concerning the Agency management structure and hierarchy you raised in your summary of your findings, top leadership needs to address these concerns. Specifically, that the "Agency lacked a management oversight system that would—as a matter of course—involve the CIO" should be addressed in a concerted manner by leadership to ensure that the CIO is "at the table" in all facets of IT planning, provisioning, management, and control.

With the constant threats and malicious activities afoot in the world and the IT environment, we must remain vigilant to be proactive in our approach, and to ensure the necessary steps are taken to safeguard our valuable information resources, while minimizing vulnerabilities and risks to our corporate system assets.

NRCS is a progressive Agency in its IT approach and methodologies, and strives to continually improve its processes, procedures, and policies to ensure the integrity, confidentiality, and availability of information resources.

Recommendation #1

Establish controls to communicate Federal and Department level security guidance to field level units, and develop an oversight system to ensure compliance.

Agency Response

In Finding 1, you mentioned that the CIO "due to a variety of circumstances…did not have controls in place to affect the appropriate policies and procedures, or to monitor their implementation." Therefore, "the Agency cannot be assured of the integrity of data used…" As stated in the background information, the CIO does not have a direct line of authority to direct, control, and manage the operations of WCC. Again, this issue is a leadership call to address, mitigate, and correct as leadership deems appropriate.

NRCS already has controls in place in the form of available information, guidance, and policies to ensure that Federal, Departmental, and Agency guidance is provided to field units.

The National Information Security Handbook states in 600.4(a): A security element must be included in each IT manager's and IT employee's Performance Work Plan. A sample element is provided with the following text: "Complies with the Department of Agriculture (USDA) and Federal security laws, regulations, and policies. Ensures security training is on their Individual Development Plan and the plans for all subordinate IT staff members. Ensures that all supervised employees receive and are credited with completion of Agency-provided security awareness training. Enables employees to become familiar with security practices and policies based on their responsibilities. Incorporates security measures and practices in assigned duties."

Oversight and controls: Each manager is responsible to ensure that all security guidance is followed. Oversight is provided when the manager performs annual performance reviews of IT personnel or other staff with major IT responsibilities. The National IRM Manual, Part 515 – Information Resources Management Reviews, Section 515.4 Responsibilities, paragraph (a) states "The NRCS CIO will ensure that an effective information resources management review program is established and followed." In keeping with this policy, the CIO conducts reviews, on an annual basis, of a small number of randomly selected organizational units to ensure compliance with security policies and procedures.

Recommendation #2

Develop a disaster recovery plan in accordance with the Office of Management and Budget (OMB) and the National Institute of Standard Technology (NIST) requirements as part of the contingency plan, and test the complete contingency plan once it is developed.

Agency Response

NRCS has made great strides in its efforts to certify and accredit its major application systems, which include the Water and Climate Information System (WCIS). The first part of this effort includes performing a Risk Assessment, which initially identifies system vulnerabilities during the Certification and Accreditation process. A System Security Plan, as well as an IT

Contingency/Disaster Recovery Plan, are then developed. Finally, an independent System Testing and Evaluation is conducted for each major application and a Risk Mitigation Plan is prepared to address each risk identified. Risks are either mitigated or accepted as appropriate. Yearly, NRCS utilizes the NIST 800-26 Assessment Response Summary to perform annual self assessments on its major application systems developing a Plan of Action and Milestones as appropriate. The WCIS Certification and Accreditation was completed on September 30, 2004, with the IT Contingency/Disaster Recovery Plan testing being completed by April 1, 2005.

Recommendation #3

Establish a formal approval process for security plans that documents the name and title of the approving management official, the date of approval, and follow Departmental Regulations.

Agency Response

Currently, NRCS has guidance in place in the National IRM Manual in Part 502 – Security Management, which directs NRCS staff on the responsibilities of maintaining security plans, which follow the USDA Departmental Manual, DM 3140-1, directive. The formal process is outlined in this section and the Information Systems Security Program Mangers (ISSPMs) responsibilities include the oversight for, and annual review of, these plans that cover the Agency's application systems. The NRCS IRM Security Manual and the National IRM Manuals are scheduled for review and updates in accordance with current Departmental policy and NIST guidance. Both manuals will incorporate language relative to Certification and Accreditation, by December 30, 2004.

Recommendation #4

Implement procedures requiring that the security plan is reviewed, updated, and certified per NIST guidelines, and that updated plans be submitted to the Office of the CIO on an annual basis.

Agency Response

Currently, NRCS has procedures governing security plan annual reviews in the National IRM Manual in Part 502 – Security Management, which directs NRCS staff on the responsibilities of maintaining security plans. The ISSPM and Deputy ISSPMs will review and assess the security plans utilizing Agency directives and NIST guidelines, and will report to the Department on an annual basis.

The NRCS IRM Security Manual and the National IRM Manuals are scheduled for review and updates in accordance with current Departmental policy and NIST guidance. Both manuals also will incorporate language relative to Certification and Accreditation and Security Plan updates, by December 30, 2004.

Recommendation #5

Perform a Certification and Accreditation on WCIS, per OMB regulations and USDA guidance.

Agency Response

The Certification and Accreditation process was completed for WCIS on September 30, 2004.

Recommendation #6

Establish controls to ensure that the use of WCIS is reauthorized every 3 years.

Agency Response

Once Certification and Accreditation for WCIS is completed, NRCS will work on a continual basis to ensure that WCIS is reauthorized every 3 years according to USDA and NIST policies and regulations.

Recommendation #7

Complete risk assessments of WCIS that will meet NIST, OMB, and USDA requirements.

Agency Response

The NRCS security team conducted a Risk Assessment on WCIS during July 2004, and will maintain these requirements per USDA and NIST policies and regulations.

Recommendation #8

Require responsible officials to timely submit verification to the CIO that monthly vulnerability scans have been run on WCIS.

Agency Response

NRCS will update appropriate policy documents to clarify the roles and responsibilities concerning system scans. The NRCS ISSPM is the responsible official for implementing USDA and NIST policies for vulnerability scans and will ensure that scans are done on major systems, which include WCIS. A monthly report on scan activity will be reported to the CIO by the NRCS ISSPM. This action is to be completed by December 30, 2004.

Page 5

Recommendation #9

Take immediate action to correct the high- and medium-risk vulnerabilities identified by the scans, and conduct an immediate rescan to ensure that the vulnerabilities have been corrected.

Agency Response

On the two high-risk vulnerabilities identified by the scanning software: a) one was found to be a false positive indicating the vulnerability did not exist, and b) the second high-risk vulnerability involved the presence of system services, which are required to meet a business requirement and function of WCIS. This vulnerability was mitigated by ensuring that no shell interpreters were in the root/cgi-bin, in accordance with accepted security practices, and this mitigation was in place at the time of the scans. On the medium vulnerability, it also involved the existence of a required service running on the e-mail server. This e-mail server has been patched to mitigate this medium vulnerability.

The NRCS ISSPM will continue to monitor scan activities and correct deficiencies, as necessary, to improve the security controls for all systems, which include WCIS. Activity reports are to be provided to the CIO on a monthly basis by the NRCS ISSPM.

Informational copies of this report have been distributed to:

Government Accountability Office (2)
Office of Management and Budget (1)
Office of the Chief Financial Officer
  Director, Planning and Accountability Division (1)